Basis Representation Theorem - Alternate Proof

James Philip Rowell

January 3, 2019 (v01)

Basis Representation Theorem

Let b be a positive integer greater than 1.

For every positive integer n there is a unique sequence of integers $d_0, d_1, d_2, \ldots, d_k$ such that:

$$n = d_k b^k + d_{k-1} b^{k-1} + \cdots + d_2 b^2 + d_1 b^1 + d_0 b^0,$$

where $0 \leq d_i < b$ for all i in $\{0, 1, 2, \ldots, k\}$ and $d_k \neq 0$.

Definition: n is represented in base-b by the string of base-b-digits $(d_k d_{k-1} \cdots d_2 d_1 d_0)_b$

The paper "Counting" proves the "Basis Representation Theorem" by induction but suggests that it could also be proven by generalizing the technique used in exercise 2-iii; that proof follows.

Lemma

Let b be an integer such that $b \neq 0$ and $c_0, c_1, c_2, \ldots, c_n$ be a sequence of integers, then:

$$(((\ldots(((c_0)b+c_1)b+c_2)b+\ldots c_{n-2})b+c_{n-1})b+c_n) = c_0 b^n + c_1 b^{n-1} + c_2 b^{n-2} + \ldots + c_{n-2} b^2 + c_{n-1} b^1 + c_n b^0$$

Proof of Lemma

QED

Euclidean Division Theorem

For all integers a and b such that $b > 0$, there exist *unique* integers q and r such that*:

$$a = qb + r \text{ such that } 0 \leq r < b$$

Definition: In the above equation:

a is the *dividend*	("the number being divided")
b is the *divisor*	("the number doing the dividing")
q is the *quotient*	("the result of the division")
r is the *remainder*	("the leftover")

*Aside: Actually the theorem is stronger than we have stated here. Specifically, it only requires that $b \neq 0$, however, to keep the remainder positive, the restriction on r would have to be stated like this $0 \leq r < |b|$ to deal with the possibility that b might be negative.